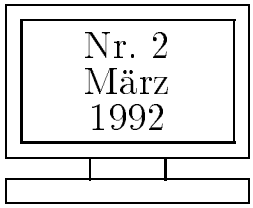
Mitteilungen Des URZ



Technische Universität Chemnitz

TU Chemnitz
Universitätsrechenzentrum
Str. der Nationen 62
O-9001 Chemnitz
kommissarischer Leiter:
Prof. U. Hübner
E-mail:
huebner@hrz.tu-chemnitz.de

Redaktion:
Dipl.-Math. Ursula Riedel
Tel.: 668 425
E-mail:
u.riedel@hrz.tu-chemnitz.de

THEMEN

In eigener Sache

Mehrere haben schon gefragt, wo sie denn bleibt, die nächste Ausgabe unserer Mitteilungen des URZ. Leider ist es mir nicht gelungen, in der stressigen Zeit vor und nach Weihnachten genügend Beiträge aufzutreiben oder zu verfassen. Die Nr. 1 1992 ist unser recht umfangreicher Jahresbericht, der aus drucktechnischen Gründen leider auch erst Ende März ausgeliefert werden kann. Aber nun ist sie endlich fertig – die Nr. 2 1992 – und hoffentlich informativ für alle Leser. In Zukunft wollen wir versuchen, im Normalfall zweimonatlich Sie mit den neuesten Informationen zu versorgen. Sollten Sie Wünsche oder Vorschläge haben, was Sie in unserem Mitteilungsblatt gern lesen möchten (natürlich nur, was zum Thema paßt), dann schicken Sie mir ein elektronisches Briefchen oder rufen Sie an (E-mail und Telefon s.o.).

Ursula Riedel

Neues vom Netz

Eine wichtige Etappe für den planmäßigen Ausbau des Universitätsnetzes wurde im vergangenen Jahr mit der Grobprojektierung und Antragstellung beim Land eingeleitet. Für den Ausbau des Netzes werden in den kommenden drei Jahren voraussichtlich entsprechende Mittel bereitgestellt. Um die „wild wuchernden“ lokalen Netze möglichst schnell an den Universitätsbackbone und damit auch an das Wissenschaftsnetz (WIN) anschließen zu können, haben wir als Vorstufe die Realisierung von ca. 10 Etagenknoten im Bereich Reichenhainer Straße/Straße der Nationen in Angriff genommen. Die Konzentration auf diese Gebäudekomplexe hat ganz pragmatische Gründe. Eine Querverbindung existiert (für alle anderen Universitätsteile sind Schaltaufträge bei der TELEKOM) und an diesen beiden Punkten ist die lokale Vernetzung schon relativ weit fortgeschritten.

Die Ausführung der Etagenknoten erfolgt so, daß die „Zwischenlösung“ sich möglichst reibungslos in das Zielprojekt einbinden läßt. Bis zu den Etagenknoten wird in Glasfasertechnik verkabelt. Der Etagenknoten ist ein Multiportrepeater (MiniMMAC), an den dann 6-12 ThinWire-Ethernet-Segmente angeschlossen werden können. Die Verteilung der Knoten erfolgt so, daß wir möglichst viele Fachbereiche und dort möglichst viele Studenten und Wissenschaftler erreichen. Wir möchten Sie deshalb hiermit auch nochmals bitten, uns mölichst früh über existierende und geplante lokale Netze zu informieren — nur so können wir diese berücksichtigen und eventuelle Anschlußprobleme vermeiden.

Folgenden Knoten entstehen dabei:

- Reichenh: MB3 – bereits realisiert
- Reichenh: Physik – bereits realisiert
- Reichenh: Elektrotechnik/Infotech – hier werden in einem abgestimmten Projekt 3 Etagenknoten realisiert
- Reichenh: Elektrotechnik/Autotech – geplant
- Reichenh: MB2 – bereits realisiert
- Reichenh: Wiwi/Rechtsw – bereits realisiert
- StraNa: Informatik – bereits realisiert
- StraNa: URZ – bereits realisiert
- StraNa: MB1 – bereits realisiert
- StraNa: Chemie – geplant

TELEKOM-Termine:

- Standleitung Scheffelstraße: 20.2.1992
- 64 KBit-WIN-Anschluß: 1.5.1992

Letzte Meldung: Seit dem 10.2.92 wird eine der zwei Leitungen zwischen der Reichenhainer Straße und Straße der Nationen mit 128 KBaud betrieben.

Günther Fischer
Ltr. Gruppe Datenkommunikation

Obelix und kein Asterix ?
Das ist nun vorbei !

Obelix, der zentrale Netzserver des Rechenzentrums, hat Verstärkung bekommen: den ***asterix***. Genau wie der „Große“ ist ***asterix*** eine HP 9000/832 Workstation und mit 16 MByte RAM und ca. 670 MByte Platte auch recht stattlich ausgerüstet. Dazu ist er von Haus aus sehr kommunikativ, Ethernet- und X.25-Karte sind an Bord. Auf ihm läuft HP-UX 8.0, HP's neueste UNIX-Version, natürlich mit TCP/IP und X.25 Unterstützung sowie – neu für HP – mit shared libraries.

Damit bietet er eigentlich alle Voraussetzungen, um die Netzdienste näher an die Nutzergemeinde zu bringen. ***Asterix*** hat seinen Standort in der Reichenhainer Straße 39 bezogen und wird als Netzserver die lokalen Netze der hier angesiedelten Fachbereiche (Mathematik, Wirtschafts- und Rechtswissenschaften, ...) mit dem Universitäts-Backbone verbinden. Das erfolgt mit einen 64 kBit/s Anschluß an die X.25 Untervermittlung in der Reichenhainer Straße 70, über die die TCP/IP Protokolle betrieben werden. Damit ist natürlich auch der Zugang zum WIN und zum Internet gegeben.

Die Kommunikationsdienste, wie electronic Mail (*elm*) und News (*nn*) sowie *telnet*, *ftp* usw. sind für diese Bereiche somit vor Ort nutzbar.

Die Beantragung eines Nutzerkennzeichens für ***asterix*** geschieht in der üblichen Weise bei Frau Pudlat, Straße der Nationen, Zi. R017. Wir empfehlen den Nutzern der Fachbereiche Mathematik sowie Wirtschafts- und Rechtswissenschaften (Reichenhainer Str. 39/41), die schon ein Nutzerkennzeichen am ***obelix*** haben, dieses auf den ***asterix*** umstellen zu lassen. Melden Sie sich bitte dafür per Email (richter@hrz.tu-chemnitz.de) oder Telefon (668 423) bei uns!

Frank Richter
Gruppe Datenkommunikation

Zum Neukauf von Software

Nach dem Senatsbeschluß vom 19.12.1991 über die „Verwaltungs- und Benutzungsordnung für das Universitätsrechenzentrum“ ist das URZ — neben der Beratung und Unterstützung in allen Softwareanwendung betreffenden Dingen — für die Beschaffung von DOS-Standard-Software zuständig. Insbesondere die einheitliche, aktuelle Ausstattung der PC-Pools für die Ausbildung erfolgt entsprechend unseren Möglichkeiten. Da wir für diesen Zweck jedoch voraussichtlich nur über geringe Haushaltmittel verfügen werden, sind wir auf die Beantragung und Zuweisung zentralisierter Gelder bei der Landesregierung angewiesen.

Im Moment ist noch offen, ob und wann und in welcher Höhe in diesem Jahr eine solche Möglichkeit besteht. Es ist jedoch ratsam, daß die Poolverantwortlichen in den Fachbereichen langfristig ihren Softwarebedarf für das Wintersemester 1992 planen und uns mitteilen. Wenn eine Finanzierungmöglichkeit besteht, kann dann schnell die entsprechende Software gekauft werden. Die Bedarfsanforderungen sollten bis Anfang Mai im URZ vorliegen. Wegen der dargestellten Randbedingungen kann von uns leider keine Garantie übernommen werden, daß die betreffende Software bis zu einem bestimmten Zeitpunkt eingetroffen ist!

Dr. Wolfgang Riedel
Ltr. Gruppe Anwendungen

Verfügbare Campuslizenzen

Das URZ verfügt gegenwärtig über drei Campuslizenzen für Softwareprodukte. Dabei handelt es sich um

- PC-ISP (keine Beschränkung)
- deLite (keine Beschränkung)
- WordPerfect (Beschränkung auf 500 Installationen)

Währenddessen wir für das System WordPerfect eine 500er Schullizenz verwalten (d.h. die Software kann innerhalb der TU maximal 500x installiert werden), sind zu PC-ISP und deLite echte Campuslizenzen vorhanden, d.h. keine zahlenmäßige Beschränkung der Nutzung.
Interessenten an solcher Software wenden sich bitte mit einem formlosen Antrag und der entsprechenden Menge formatierter Disketten (siehe unten) an Dr. W. Riedel, Zimmer 1/363e, Telefon 668422.

WordPerfect

Das System umfaßt im Einzelnen die folgende Software:

WordPerfect 5.1	Textverarbeitung (deutsche Version)
PlanPrefect 5.1	Tabellenkalkulation (englische Version)
DrawPerfect 1.1	Grafikpaket (englische Version)
DataPerfect 2.1	Datenbank (englische Version)
WordPerfectOffice LAN 3.0	Netzwerk/Kommunikationsprogramm (englische Version)

Die Lizenz wird an alle Interessenten innerhalb der TU vergeben, die Software darf auf allen Uni-eigenen Rechnern eingesetzt werden. Es ist für jeden Rechner (auch innerhalb eines Netzes) eine Lizenz notwendig. Folgende Voraussetzungen sollten für eine erfolgreiche Nutzung erfüllt sein: MS DOS 3.0 oder höher, 640 KB RAM (zusätzlicher Expansionsspeicher ist empfehlenswert), ca. 14 MB Festplattenplatz. Die Übergabe erfolgt auf 11 3.5″-Disketten (1.44 MB) oder 24 3.5″-Disketten (720 KB) oder 44 5.25″-Disketten (360 KB). Der Diskettenbedarf und der notwendige Festplattenplatz für die einzelnen Komponenten des Systems können nachfolgender Tabelle entnommen werden.

	3.5″ 1.44 MB	3.5″ 720 KB	5.25″ 360 KB	Festplatte MB
WordPerfect	3	7	13	4
PlanPerfect	3	6	11	3
DrawPerfect	3	6	12	3,5
DataPerfect	0,5	1	2	0,5
WordPerfectOffice	1,5	4	6	3

Interessenten an WordPerfect & Co. stellen bitte einen formlosen Antrag (Uni-Kopfbogen, Anzahl der gewünschten Lizenzen, Gerätenummern — die Lizenzen sind aus rechtlichen Gründen maschinenbezogen —, Adresse eines verantwortlichen Bearbeiters, Unterschrift) an das URZ. Bei der Rückgabe der bespielten Disketten wird durch Unterschrift eine kurze Vereinbarung

über die Lizenzweitergabe zwischen dem URZ und dem betreffenden Fachbereich bzw. Dezernat oder Abteilung abgeschlossen. Außerdem erhalten Sie eine Anleitung zur Installation. Dokumentationen zu allen Teilen der WordPerfect-Software sind mittlerweile durch das URZ gekauft worden. Allerdings ist dabei zu beachten, daß diese nur in beschränktem Umfang zur Verfügung stehen. Entsprechend den bisher ausgegebenen Lizenzen von WordPerfect wurde den Fachbereichen Literatur im Verhältnis 1:10 (*WordPerfect Arbeitsbuch*) bzw. 1:15 (*WordPerfect Nachschlagen*) übergeben. Die Computerverantwortlichen müssen die sinnvolle Aufteilung und Nutzung dieser Bücher in ihrem Fachbereich organisieren.
Aktuellere Ausgaben der Software (deutsche Versionen für alle Teile, WordPerfect für Windows, WordPerfect für UNIX u.dgl.) stehen kurzfristig nicht zur Verfügung. Bei einem größeren Bedarf innerhalb der TU müßten solche Updates gekauft werden (s. Beitrag „Neukauf von Software “, S. 4).

PC-ISP/DGS+ Version 3.1

Bei dieser Software der Firma Datavision (Klosters, Schweiz) handelt es sich um ein Datenanalyse- und -auswertungssystem. *I*nteractive *S*cientific *P*rocessor ist eine spezielle Programmiersprache, die interpretativ abgearbeitet wird. Man kann aus Grundobjekten (Zahlen, Strings, Namen, Felder) mathematische Formeln bilden, diese manipulieren, auswerten und grafisch darstellen.
Das System ist in zwei Konfigurationen vorhanden:

- die „personal“–Version verlangt einen PC 80286, EGA oder VGA, Microsoft-kompatible Maus, DOS 3.3 oder höher,
- die „386er“–Version erfordert einen PC 80386(SX) und einen 80387(SX)-Koprozessor, mindestens 2MB extended RAM, EGA oder VGA, MS-kompatible Maus, DOS 3.3 oder höher.

Beide Versionen benötigen nur 2 MB Festplattenplatz.
Die Übergabe der Software erfolgt für die „personal“–Variante auf einer, für die „386er“–Version auf zwei 3,5″ HD-Disketten.
Ein Handbuch zu PC-ISP ist im URZ zur Ausleihe vorhanden. Im Moment bemühen wir uns um eine globale Kopiergenehmigung und dazu ein kopierfähiges Handbuchexemplar.

deLite Version 2.01

Diese Software der Firma BrainLab (Berlin) stellt eine grafische Toolbox für TurboPascal 6.0 dar. Man kann damit die Oberfläche von Anwendungen einfach programmieren (Pulldown-Menüs, Mausbedienung, kontextsensitive Hilfefunktionen, objektorientierte Dialoge u.a.). DeLite selbst ist in TurboPascal 6.0 geschrieben und besteht aus 2 Units, die vom Anwenderprogramm importiert werden müssen.
Empfohlene Hardwarevoraussetzungen: 1 MB Festplattenplatz (temporär), Maus, EMS.
Die Übergabe erfolgt auf einer 5.25″ Diskette. Ein ungebundenes Handbuch wird zum Kopieren ausgeliehen (Kopiererlaubnis explizit vorhanden).

Dr. Wolfgang Riedel
Ltr. Gruppe Anwendungen

Kostenfreie Software

Neben der Beschaffung von Campuslizenzen bemüht sich das URZ um die Erschließung von kostenfreier Software (vom Public Domain Server der TUCh), da sich damit für alle TU-Mitarbeiter Möglichkeiten zur kostengünstigen Nutzung der verschiedensten Software eröffnen. Man kann mittlerweile davon ausgehen, daß für die meisten der kommerziell vertriebenen Softwareprodukte funktionsgleiche, kostenlose Äquivalente existieren. Die Menge der auf internationalen Servern gesammelten kostenfreien Software ist aber derartig umfangreich, daß das Bereitstellen und gezielte Anbieten nur schrittweise und für ausgewählte Schwerpunkte erfolgen kann. Wir werden in den „Mitteilungen des URZ“ von Zeit zu Zeit über den aktuellen Stand dieser Erschließungsarbeiten berichten.

Bereits große Erfahrungen gibt es bei verschiedenen TU-Mitarbeitern bei der Anwendung des Satzsystems TEX bzw. LATEXDiese Software ermöglicht professionelle Textverarbeitung einschließlich Formel-, Tabellen- und Grafikgenerierung bis hin zur professionellen Layout-Gestaltung. Verschiedenste Schriftformen, -arten (auch kyrillisch, arabisch usw.) und Sonderzeichen (z.B. für Musiknoten) sind vorhanden. Vorhandene Grafiken unterschiedlicher Formate (TIFF, PCX, IMG, GIF usw.) können eingebunden werden.

TEX bietet den großen Vorteil, daß es funktionsgleich für DOS und UNIX verfügbar und – da kostenfrei – frei kopierbar ist. Interessenten wenden sich bitte an Dr. W. Riedel (Zi. 1/363e, Tel. 668422). Zur Übergabe der DOS-Version *emTeX* sind ca. 10 HD-Disketten (3.5″) erforderlich; die genaue Anzahl hängt von den zu installierenden Druckertypen ab.

Die Generierung und Installation einer UNIX-Version auf Ihrer Maschine bieten wir als Service an, dazu sind konkrete persönliche Absprachen notwendig.

Auf allen dem URZ gehörenden Workstations und im PS/2-ABZ ist TEX installiert.

Dr. Wolfgang Riedel
Ltr. Gruppe Anwendungen

Nutzung von Vektorrechnern

Zur Lösung umfangreicher numerischer Berechnungen werden international in zunehmendem Umfang Supercomputer eingesetzt. Zu dieser Rechnerklasse gehören die sogenannten Vektorrechner. Diese besitzen einen speziellen Prozessor, der Maschinenbefehle für Vektoroperationen ausführen kann. Ein Vektor wird dabei als Menge von Zahlen gleichen Typs betrachtet (Gleitpunktzahlen), die im Speicher sequentiell aufeinanderfolgend stehen müssen. Auf alle Elemente eines solchen Vektors wird die gleiche arithmetische Operation angewendet. An der TU Dresden steht ein Rechner IBM 3090-200 (mit Vektoreinrichtung) zur Verfügung, der auch von Wissenschaftlern unserer Einrichtung genutzt werden kann. Der Zugriff ist über Netz möglich. Auf der genannten Anlage ist auch die FORTRAN-Programmbibliothek „Engineering and Scientific Subroutine Library“ (ESSL) verfügbar.

Im Oktober 1991 wurde in Dresden außerdem der „Landesvektorrechner Siemens VP200“ übergeben. Auch mit dieser Maschine kann in der beschriebenen Weise gearbeitet werden. Interessenten an diesen Möglichkeiten melden

sich bitte bei Dr. W. Riedel (Zi. 1/363e, Tel. 668422).

Demo-Disketten

Das URZ verfügt über eine größere Anzahl von Demo-Disketten für Software der verschiedensten Sachgebiete. Diese Disketten können von allen Interessenten für die eigene Information ausgeliehen werden.

Bezeichnung d. Software	Sachgebiet	Firma	Disk. typ
Statistica	Statistik	IMS	3.5″
Mathematica	mathem. Formelauswertung	IMS	3.5″
Mathematica	mathem. Formelauswertung	Additive	3.5″
T3	Textverarbeitung	IMS	3.5″
Axum		IMS	3.5″
WordPerfect für Windows	Textverarbeitung	WordPerfect	3.5″
PageMaker	DTP	Aldus	3.5″
CorelDraw	Zeichenprogramm		3.5″
PrismaOffice	Bürosystem	electronic Lichtenstein	3.5″
Autosketch 3.0			5.25″
WindowBase		SPI	5.25″
Modula-2	Programmiersprache	SWD	5.25″
NumLib	Numerische Bibliothek für Modula-2	Miele/Roland	5.25″
Quickstep-Tools		Lauer & Wallwitz	5.25″
Windows Tools		Borland	5.25″
Excel 3.0 für Windows	Integrierte Software	Microsoft	5.25″
Science & Engin. Tool		Quinn Curtis	5.25″
Vermont Views		Vermont Creative Software	5.25″
View232		Blaise	5.25″
QickStep Tools		Lauer & Wallwitz	5.25″
ToolTec Views		Ing.-Büro Röther	5.25″
Structor		Basis Institut	5.25″

Bezeichnung d. Software	Sachgebiet	Firma	Disk. typ
Menuet Dev.Ed.		Ithaca Street	5.25″
Graphics-Menue		Island Systems	5.25″
QNX	Echtzeit-Betriebssystem	SWD	5.25″
SWD-Expert	Echtzeit-Expertensystem	SWD	5.25″
PRO-RENO	Kanzleiprogramm	MSD	5.25″
INKS	Kaufmännische Software	MSD	5.25″
Kfz-Pilot	Branchensoftware	MSD	5.25″

Dr. Wolfgang Riedel
Ltr. Gruppe Anwendungen

Computerviren: Eine Einführung

Begriffsbestimmungen

Eine sehr einfache Definition dessen, was ein Computervirus ist, könnte sein:

> *Ein* Virus *ist ein Programm(stück), das andere Programme modifiziert, indem es eine Kopie von sich selbst in diese plaziert.*

Diese Definition ist etwas vereinfacht, zeigt aber ausreichend den Hauptunterschied zwischen Viren und anderen Schadprogrammen wie den sogenannten „Trojanischen Programmen“ oder „Würmern“.

> *Ein* Trojanisches Programm *ist ein Programm, das etwas nützliches (oder wenigstens interessantes) zu tun vorgibt, in Wirklichkeit bei seiner Ausführung jedoch im verborgenen einige vom Benutzer nicht erwünschte (meist schädliche) Funktionen ausführt.*
>
> *Ein* Wurm *ist ein Programm, das seine eigene Verbreitung in Netzen organisiert, ohne daß eine Kopplung an andere Programme besteht.*

Viren und Trojanische Programme können „Zeitbomben“ enthalten. Unter Zeitbomben werden solche Schadfunktionen verstanden, die erst beim Eintreten bestimmter Bedingungen (z.B. einem bestimmten Datum) ausgeführt werden.
Schadfunktionen sind bisweilen Funktionen, die großen Schaden verursachen, wie z.B. das Formatieren der Festplatte. Oft sind die Störungen jedoch auch relativ harmlos, z.B. nur das Abspielen einer Melodie oder eine Bildschirmausgabe.

Bei Viren lassen sich funktionell vier Komponenten feststellen:

1. Ein Programmstück, das die Weiterverbreitung des Virus besorgt.

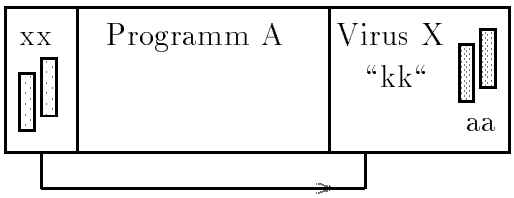
2. Eine „Kennung“, durch die der Virus erkennt, ob ein File schon von diesem Virustyp infiziert ist.
3. Beliebige zusätzliche Funktionen (Schadfunktionen!).
4. Der Aufruf des eigentlichen Trägerprogramms.

Gelegentlich wird dafür geworben, die Techniken der Virenprogrammierung für positive Zwecke einzusetzen, denn die oben erwähnten beliebigen Funktionen im Virus brauchen nicht notwendigerweise Schadfunktionen sein. Jedoch kann es aus prinzipiellen Erwägungen heraus keine „harmlosen“ Viren geben. Selbst wenn keine Zerstörungen vorgesehen sind, ist allein die „Einmischung“ des Virus in die Arbeit der Anwendungsprogramme (Verbiegen von Interruptvektoren, Verlangsamung des Rechners, Speicherbelegung usw.) eine Störung, die erheblichen Schaden verursachen kann (z.B. bei Produktionssteuerungen). Außerdem kann durch unbeabsichtigte Programmmierfehler oder durch absichtliche Modifikationen daraus leicht ein gefährliches Programm werden.

Woher kommen Viren? Wie funktionieren sie?

Viren werden (wie andere ausführbare Programme auch) von Menschen erzeugt, die die Idee dazu haben und umsetzen können.
Jeder durchschnittlich begabte Assemblerprogrammierer kann leicht ein derartiges Programm schreiben, doch bieten auch die modernen höheren Programmiersprachen mit ihren Betriebssystemschnittstellen gute Voraussetzungen für solche Absichten.
Viren können in beliebigem ausführbaren Programmcode eingebaut sein: Im Bootsektor, in Gerätetreibern, in normalen Maschinenprogrammen, in Überlagerungsfiles. Theoretisch ließen sich auch Viren auf der Shell-Ebene erzeugen, doch ist dies aus Sicht der Virenprogrammierer wegen der größeren Entdeckungsgefahr wenig effektiv.
Auf PC's treten hauptsächlich zwei Typen von Viren auf: *Bootsektorviren* und *Programmviren*.
Arbeitsweise eines Programmvirus (vereinfachtes Beispiel):

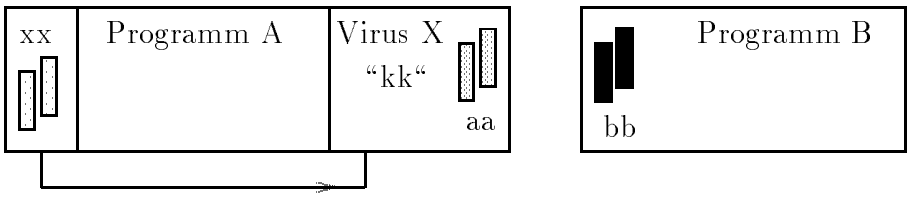
1. Ein mit einem Virus X infiziertes Programm A wird aufgerufen.
   Nachdem es vom Betriebssystem geladen wurde, steht es wie folgt im Hauptspeicher:



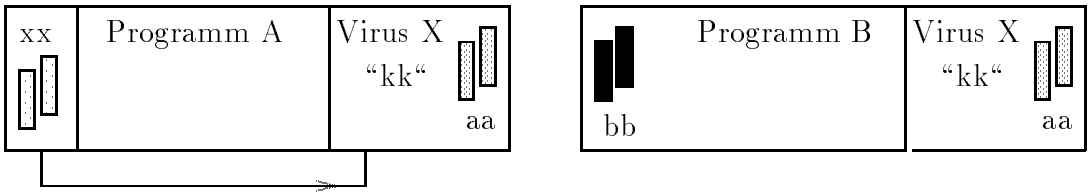
2. Am Anfang steht ein Sprungbefehl zum Anfang des Virus.
   Der Virus führt seine Arbeit also vor dem Programm aus.

3. Der Virus X schaut im aktuellen Verzeichnis oder in anderen Verzeichnissen nach geeigneten Programmen, die noch nicht vom Virus X infiziert sind. Dazu testet er, ob die Programme seine Kennung **kk** enthalten.

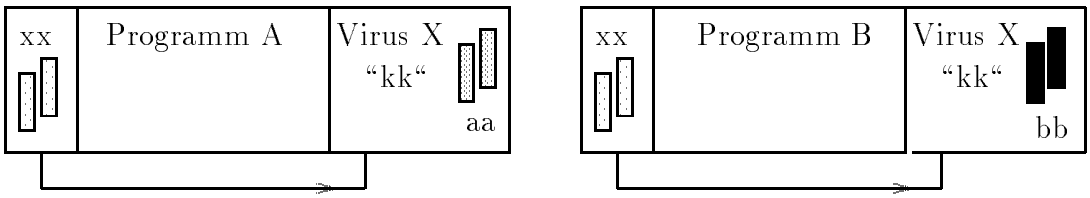
4. Ein noch nicht infiziertes Programm B wird gefunden und in den Hauptspeicher geladen:



5. Der Virus überträgt seinen Code hinter das Programm B:



6. Der Virus sichert die ersten Bytes vom Anfang des Programms B in den Datenbereich seiner Kopie, schreibt danach einen Sprungbefehl in den Anfang des Programms B:

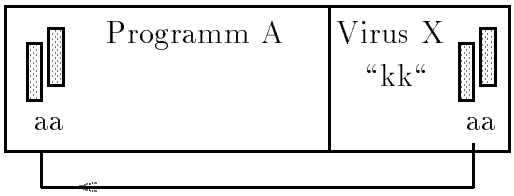


7. Der Virus schreibt das so modifizierte Programm B unter dessen alten Verzeichniseintrag (B) zurück. Damit ist B infiziert und würde bei einem späteren Aufruf mit den gleichen Operationen beginnen, die bis hierher vom Virus X ausgeführt wurden.

8. Je nach „Ansteckungsgrad“ des Virus können jetzt die Schritte 3 bis 7 für weitere, noch nicht infizierte Files durchgeführt werden.

9. Sollen bzw. können keine weiteren Programme infiziert werden, folgt jetzt die Ausführung der sonstigen Funktionen des Virus (Schadfunktionen).

10. Hat der Virus seine sonstigen Funktionen beendet, werden im Hauptspeicher die ursprünglichen Byteinhalte am Programmanfang wiederhergestellt. Damit steht das Programm A so im Speicher wie es normalerweise ohne den Virus geladen worden wäre:



11. Der Virus beendet seine Arbeit, indem er an den Anfang des Programms A springt.

12. Das Programm A beginnt seine Arbeit. Ob es unter den gegebenen Bedingungen noch ordnungsgemäß arbeiten kann, ist ungewiß.

Bootsektorviren nisten sich im Bootsektor der Festplatte oder von Disketten ein (auch Datendisketten ohne Programme). Wird von einem solchen Datenträger gebootet oder versucht

zu booten, so übernimmt der Virus sofort die Steuerung des Rechners und versteckt sich im Hauptspeicher. Danach lädt er vom Datenträger den originalen Bootsektor, der von ihm irgendwo anders abgespeichert worden ist, und läßt ihn ausführen, wonach alles scheinbar wie gewöhnlich abläuft, außer daß natürlich danach jede Diskette, die nicht schreibgeschützt ist, von ihm aus dem Hintergrund heraus infiziert wird. Das „Verstecken“ im RAM wird gewöhnlich so realisiert, daß die Menge des Speichers reduziert wird, die DOS zur Verfügung steht, z.B. ein PC mit 640K RAM erscheint dann so, als ob er nur 639K hätte.
Der Virus bleibt solange im Hauptspeicher aktiv, bis der Rechner ausgeschaltet wird. Ein Booten nur mit Ctrl-Alt-Del (Warmstart) überleben einige dieser Viren.
Die Methode der hauptspeicherresidenten Installierung tritt auch bei Programmviren sehr häufig auf. Diese Viren infizieren dann andere Programme nicht nur beim Start eines verseuchten Programms, sondern sind in der Lage, jedes File, das irgendwann behandelt wird (auch bei nur Lesen), zu infizieren.
Abschließend sollen noch einige häufige Mißverständnisse darüber korrigiert werden, welche Gefahren nicht von einem Virus ausgehen:

- Ein Virus kann nicht von einem Computertyp (z.B. IBM kompatibler PC) auf einen völlig anderen (z.B. AMIGA) übertragen werden.
- Ein Virus entsteht nicht von allein, er muß wie jedes andere Programm geschrieben werden.
- Nicht alle Viren wirken sich katastrophal aus. Manche verursachen nur geringe Behinderungen.
- Ein Rechner kann nur infiziert werden, wenn entweder von einer infizierten Diskette gebootet wird, oder wenn ein infiziertes Programm auf ihm ausgeführt wird. Lesen von einer infizierten Diskette kann nicht zur Infizierung führen.
- Eine schreibgeschützte Diskette kann nicht infiziert werden.
- Viren können nicht aus Datenfiles aktiv werden.

Gegenmaßnahmen

a) Schutzmaßnahmen gegen bekannte Viren:

- *Virenscanner*: Überprüfung aller relevanten Files, ob in ihnen bekannte Virenkodes enthalten sind. Zahlreiche Programme dieses Typs sind im Angebot (z.B. SCAN von McAfee). Probleme dabei:
  1) nur erforschte Viren können gesucht und gefunden werden;
  2) laufende Updates der Scan-Programme sind notwendig;
  3) Spektrum der bekannten Viren differiert bei Scan-Programmen.

  Vorteilhaft: Für zahlreiche erkannte Viren gibt es Gegenmittel, die aus den infizierten Programmen die Originalprogramme wiederherstellen können.
- *Programmschutz durch Vortäuschen einer Infektion*: Wenig sinnvoll. Stammt noch aus der Anfangszeit der Virenplage, als es nur sehr wenig Viren gab. Gegenwärtig liegt bei MS-DOS die Anzahl bekannter Viren bei über 1000 (mit Varianten), davon sind noch nicht alle genau erforscht.
- *Online-Kontrolle*: Jedes auszuführende Programm wird während des Ladens auf bekannte Virenkodes überprüft. Dazu werden spezielle speicherresistente Utilities verwendet.

b) Schutzmaßnahmen gegen unbekannte Viren:

- *Prüfsummenalgorithmen*: Regelmäßig werden von allen relevanten Files Prüfsummen berechnet und in Listen abgespeichert. Die Listen werden mit denen aus früheren Prüfsummenbildungen verglichen. Verdächtige Veränderungen müssen genauer überprüft werden. Auch der Bootsektor muß in den regelmäßigen Vergleich einbezogen sein. Diese Methode ist als wahrscheinlich sicherste anzusehen. Wichtig ist bei dieser Maßnahme, daß dazu der Rechner unbedingt von einer garantiert virenfreien Systemdiskette gebootet werden muß, um während der Arbeit des Prüfsummenprogramms nicht unabsichtlich weitere Vireninfektionen zu bewirken.
- *Zugriffsschutz durch Überwachung der Laufwerkzugriffe*:
  Die Festplatten-/Diskettenzugriffe werden überwacht. Bei dem Versuch, auf Files zu schreiben, ist ein Bedienereingriff erforderlich. Probleme dabei:

  1. Wird von machen Viren umgangen;
  2. Fehlende Kenntnisse des Benutzers, ob die angeforderte Erlaubnis gegeben werden soll oder nicht;
  3. gewisse Behinderung der Arbeit.

c) ungeeignete Schutzmaßnahmen:

- Für alle Files das Readonly-Attribut setzen;
- Umbenennen von Files;
- Verstecken von Files (z.B. COMMAND.COM) in Subdirectories.

d) allgemeine Schutzvorkehrungen:

- Keine unbekannten Programme starten; fremde Programme und Disketten erst checken.
- Disketten nur schreibgeschützt benutzen.
- Nicht von fremden Disketten booten. Falls beim Start des Rechners eine Diskette im Laufwerk A: war, ausschalten und ohne Diskette neu booten.
- Regelmäßige Überprüfungen des Typs a) oder b) ausführen. Dafür sollte stets von einer speziell dafür vorgesehenen, garantiert virenfreien, schreibgeschützten Diskette gebootet werden.
- Rechtzeitiges Erstellen von Backup-Kopien der eigenen Programme (vor der Benutzung und nur in einem virenfreien System). Sicherungsdisketten danach nur schreibgeschützt verwenden.
- Obacht geben auf ungewöhnliches Verhalten von Programmen oder Rechnern.
- Vireninfektionen nicht verschweigen, sondern kompetente Spezialisten hinzuziehen und Kontaktpartner informieren.

Verhaltensweisen und Arbeitsschritte bei Virenbefall

Vorbemerkung:
Ein Computervirus meldet sich in den seltensten Fällen mit „Hausnummer und Adresse“ beim Nutzer eines verseuchten Systems. In allererster Linie wird man als Computernutzer durch

ungewöhnliche Reaktionen bei der Abarbeitung von Software, die von der bisherigen und gewohnten Arbeitsweise der Programme erheblich abweichen, auf einen eventuellen Virus in der Software aufmerksam. Andererseits ist nicht jede ungewohnte Reaktion eines Programms bzw. Störung bei der Programmabarbeitung die Wirkung eines Computervirus, sondern kann das Ergebnis einer Fehlbedienung, einer fehlerhaften Daten- oder Programmdatei oder einfach das Ergebnis einer in der Zwischenzeit durch einen mitbenutzenden Kollegen durchgeführten Veränderung der Standardparameter einer Software sein.
Hier ist also in jedem Fall erst einmal ruhiges und besonnenes Handeln des Computernutzers unbedingt erforderlich. Übereiltes Handeln, wie zum Beispiel das Löschen eines vermeintlich „virenverseuchten" Programms, ohne genaue Kenntnis bzw. Nachweis eines Computervirus, führt zu unnützer Mehrarbeit und Verzögerung bzw. Behinderung der weiteren Arbeit mit dem Computer und bietet auch keine Garantie, daß das Gerät dann „sauber" ist, d.h. der Virus eliminiert ist.
Handlungen des Nutzers bei begründeten Verdacht auf Viren:

1. Keine übereilten oder überhasteten Reaktionen. Ruhiges und besonnenes Handeln ist geboten. Das bedeutet, erst einmal alle laufenden Arbeiten sofort einstellen.
2. Alle Disketten, mit denen gearbeitet wurde (auch in zurückliegenden Zeiten), sind vom Rechner zu entfernen und sicher aufzubewahren. Diese sind später auf virenverseuchte Programme zu überprüfen, bzw. die Datenbestände sind auf ihre Richtigkeit zu überprüfen. (Wird generell mit schreibgeschützten Disketten gearbeiten, ist diese Kontrolle überflüssig.)
3. Information des für das Gerät zuständigen Systemverantwortlichen, der evtl. die weiteren Schritte der Prüfung der Festplatte bzw. der Disketten einleitet sowie die notwendigen Informationen weitergibt.
4. Diese Schritte sollten sein:
   a) Die sofortige Prüfung der Festplatte mittels geeigneter Prüfprogramme von einer schreibgeschützten, virenfreien Diskette.
   b) Prüfung der Festplatte mit den bereitgestellten Virensuchprogrammen. Das gibt allerdings keine absolute Sicherheit, da diese Programme nur bekannte Viren lokalisieren können. Ist ein noch unbekannter Virentyp zu vermuten, sind virenbehaftete Programme auf einer Diskette zu sichern.
5. Das Gerät ist auszuschalten und anschließend mit der Original–Systemdiskette zu starten. Wichtig ist, daß alle weiteren Befehle und Aktivitäten ausschließlich von der mit einem Schreibschutzaufkleber versehenen Systemdiskette aus gestartet werden. Auf keinen Fall darf ein Programm von der Festplatte aus gestartet werden.
   Zur Beseitigung des Virus gibt es mehrere Möglichkeiten, abhängig von der Intensität des Befalls:
   a) Sind nur wenige Programme befallen, sind diese Programme zu löschen (DEL). Anschließend von den Originaldisketten (mit Schreibschutz) diese Programme neu installieren.
   b) Handelt es sich um einen der bekannten Viren, zu denen ein sogenanntes „Anti-Programm" existiert, können die infizierten Programme durch den Einsatz dieses Gegenprogramms „repariert" werden. Danach sind diese Programme wieder voll funktionsfähig. Aus den Beschreibungen der Virentypen ist ersichtlich, bei welchen Viren alle Programme hinsichtlich ihrer Funktionstüchtigkeit zusätzlich geprüft werden müssen.

c) Handelt es sich um Bootsektorviren oder sind die Mehrzahl der Programme befallen oder stehen keine aktuellen Anti-Programme zur Verfügung, empfiehlt es sich, die Festplatte neu zu formatieren und anschließend die Platte neu zu installieren. Dazu sind vorher ggf. die Datendateien, aber nur diese (keine Programme!), auf gesonderten Disketten zu speichern, um Datenverluste zu vermeiden. Diese gesicherten Dateien können nach der Neuinstallation der Platte wieder zurückgespeichert werden. Es ist aber unbedingt zu prüfen, ob Daten verfälscht oder gelöscht wurden.

6. Ausschalten des Gerätes und neu starten.

Was ist noch zu beachten:

- Es sind unbedingt alle anderen Geräte zu prüfen, ob auch sie von dem Virus befallen sind. Die Prüfung erfolgt in analoger Weise.
- Es sind alle in Frage kommenden Disketten zu überprüfen, um eine Weiterverbreitung zu verhindern.
- Wenn möglich, sind Hinweise und Erkenntnisse zur Quelle des Virus zu lokalisieren.
- Information aller Nutzer, deren Rechner möglicherweise auch infiziert wurden (Softwareübergabe).

Angebot des Universitätsrechenzentrums

- Das URZ ist bestrebt, leistungsfähige Virenerkennungs- und -beseitigungssoftware zur Nutzung anzubieten und auf dem jeweils aktuellen Stand zu halten. Gegenwärtig wird noch geprüft, ob und für welche derartigen Programme ein Campuslizenz erhältlich ist.
- Das URZ wird weitere Antivirenprogramme, die nicht über eine Campuslizenz verteilt werden können, in Reserve halten und in akuten Notfällen zur Diagnose und Therapie hinzuziehen.
- Das URZ sammelt Informationen zu eingetretenen Infektionen und gibt Hinweise zur vorbeugenden Virenbekämpfung.

Ansprechpartner im URZ:
Dipl.-Math. Alfred Pfeiffer, Zi. 1/362, Tel. 668 252. Gruppe Anwendungen

Die TU Chemnitz ist Mitglied der OSF

Was ist die „OSF“ ?

Die OSF – „Open Software Foundation“ – ist eine internationale Organisation, die sich der Entwicklung und Verbreitung einer offenen, portablen Softwareumgebung widmet. Anbieter und Nutzer haben gleichermaßen Zutritt. 1988 wurde die OSF mit Unterstützung von sieben Sponsoren der Industrie gegründet, denen weitere folgten. Die Liste der weltweit mehr als 200 Mitglieder schließt führende Computerfirmen, Softwareentwicklungshäuser, kommerzielle Endnutzer,

Forschungsorganisationen, Universitäten und Verwaltungsagenturen ein. In einem neutralen Rahmen vereinigt die OSF Anbieter, Konsumenten und Entwickler, um die industriellen Erfordernisse zu diskutieren und kooperativ den Weg für offene Systeme darzustellen.

Die OSF ist keine Standardisierungsorganisation, ergänzt jedoch deren Arbeit durch Schaffung von entsprechenden Implementationen. Die OSF arbeitet nicht profitorientiert.

Das Ziel ist es, Nutzern die Anpassung und den Einsatz von Soft- und Hardware verschiedener Anbieter zu erleichtern. Dazu ist eine anbieterneutrale Softwarearchitektur zu schaffen, bei der Computersysteme verschiedenster Anbieter in einer im wesentlichen nahtlosen Umgebung zusammenarbeiten.

Die Forderungen sind Portabilität (Anwendungssoftware auf Computern verschiedener Anbieter zu nutzen), Interoperabilität (Vereinigung von Computern verschiedener Anbieter in einem Netz) und Scalibilität (Anwendungen und Systeme auf allen Klassen von Computern nutzen, von Desktop-Workstations bis hin zu Supercomputern). Computer-Nutzer haben eine anbieterneutrale Operationsumgebung für ihre Anwendungen gefordert, was anfangs von der Industrie abgelehnt wurde.

Das „OSF Research Institute (RI)“ gilt als Verbindung der OSF einerseits und sowohl den Universitäten als auch kommerziellen Labors andererseits. Veröffentlichungen erscheinen regelmäßig als „RI NOTES“.

Den Schlüssel zum Erfolg sieht die OSF im innovativen offenen Prozeß. Dazu schreibt die OSF sogenannte „Requests for Technology (RFT)“ aus. Unter Auswertung der Ideen aller Interessenten zu technologischen und Markt-Erfordernissen sowie Empfehlungen der Mitglieder, Industrieberater, Standardisierungsgruppen u.a. wählt die OSF die Technologien für die offene Computerumgebung aus. Mitglieder erhalten rechtzeitigen Zugriff dazu durch Kopien des in Entwicklung befindlichen Codes, genannt „snapshots“. Dadurch ist ein schneller Technologietransfer zur Industrie gesichert.

Eine Reihe von Technologien offener Systeme ermöglicht den Nutzern, Software und Hardware verschiedener Anbieter zu integrieren und innerhalb einer scheinbar nahtlosen Umgebung anzupassen. Grundlage dazu ist das OSF/1^{TM}-Betriebssystem. Darüber sind gelagert

- Distributed Computing Environment (DCE), ein integriertes System von Technologien, die den Nutzern Zugriff zu verschiedenen Netzwerkressourcen vom Desktop aus erlauben.
- Grafical User Interface for Open Systems (GUI), ein Angebot, das Applikationen ein übereinstimmendes Aussehen und Verhalten auf allen Systemklassen verleiht, vom Desktop bis zu Mainframes. Das grafische Nutzerinterface Motif^{TM} fand breite Anwendung.

DCE und Motif^{TM} können sowohl unter OSF/1 als auch anderen Betriebssystemen laufen. Für die offene Computer-Umgebung ist es wichtig, die industriellen Erfordernisse zu verfolgen. Gemeinsam mit ihrer Mitgliedschaft wird die OSF sowohl erprobte als auch neu entstehende Technologien für den Einschluß in die Umgebung berücksichtigen.

Durch den „Request for Technology“-Prozeß (RFT), wurden z.B. Technologiekonzepte für eine Verwaltungsumgebung (DME) und ein architekturneutrales Verteilungsformat (ANDF) für Software erarbeitet. Die DME wird Systemverwaltung wirksamer und kosteneffektiver gestalten. Die OSF testet die Durchführbarkeit der ANDF-Technologie, die Softwarelieferer befähigen würde, Applikationen in einem einzigen Format zu verbreiten, die aber auf einer großen Breite von Hardware genutzt werden kann.

Die erforderlichen Schnittstellen für die Entwicklung portabler Applikationen für eine of-

fene Systemumgebung werden in der „Application Environment Specification (AES)“ definiert. Dieses sich entwickelnde Dokument erscheint in mehreren Bänden.

Der Hauptsitz der OSF wurde in Cambridge (USA) eingerichtet. Weitere Geschäftsstellen bestehen für Europa in München (Deutschland), Zaventem (Belgien) und Grenoble (Frankreich) sowie für Asien in Tokio (Japan).

Anmerkung

Diese Mitteilung dient ausnahmslos der Information und stellt keine Bewertung der OSF dar. Alle Informationen wurden entsprechenden Materialien der OSF entnommen.

Hinweis

Durch regelmäßige Veröffentlichungen werden die OSF-Mitglieder über den Entwicklungsstand der einzelnen Projekte informiert. Direkter Erfahrungsaustausch erfolgt in Member-Meetings und verschiedenen Formen von Kursen.

Alle vorliegenden Publikationen können im Fachbereich Informatik (bei U. Luthe, Rechnerbetriebsgruppe, Zi. 1/248, Tel. 668390) eingesehen werden.

Ulrike Luthe
Fachbereich Informatik
Rechnerbetriebsgruppe

Neues zum Kursangebot

Unser Angebot an Kursterminen für den Zeitraum Semesterpause/Frühjahrssemester 1992 ist Mitte Januar erschienen, in Form von Aushängen bzw. Informationsblättern an die Fachbereiche und zentralen Einrichtungen. Für die Mehrzahl der Kurse ist die Nachfrage so groß, daß schon Ersatzkurse geplant werden mußten. Das betrifft die Kurse *Einführung in Unix*, *Programmieren mit C*, *Programmieren mit C++*, *Nutzung des Rechnernetzes*, *X Window-System für Benutzer*, *Programmieren mit X Windows und OSF/Motif*.

Für folgende Kurse sind teilweise noch Anmeldungen möglich:

Satzsystem LaTeX	25.–27.5., 1.–3.6.92	13.00 – 18.00 Uhr
Programmieren mit C	15.06.–26.06.92	7.15 – 12.00 Uhr

Folgende Kurse sind neu im Angebot:

vi – der Editor für Electronic Mail[1]	24.4.92	8.00 – 12.00 Uhr
DOS – Einführungskurs	15.06.–19.06.92	7.15 – 12.00 Uhr
DOS für Systemverantwortliche	29.06.–03.07.92	12.30 – 17.30 Uhr

Wichtiger Hinweis

[1] Grundkenntnisse in der Texterfassung mit dem Editor *vi* sind Voraussetzung für den Kurs *Nutzung des Rechnernetzes*!

Wir bitten alle Studenten und Mitarbeiter, die sich für unsere Weiterbildungskurse eingeschrieben haben, sich eine Woche vor Kursbeginn nochmals zu melden (bei Frau Pudlat, Zi. R017, Str. der Nationen, Tel. 668656, Email: r.pudlat@hrz.tu-chemnitz.de oder, wenn dort niemand erreichbar ist, bei Frau Riedel, Tel. und Email s. Seite 1). Sehr wichtig ist das besonders bei den stark belegten Kursen, wo wir oft Ersatzkurse anbieten müssen, um die Qualität zu erhalten. Leider ist es mitunter so, daß sich Interessenten sehr zeitig anmelden und sich dann nicht mehr melden bzw. nicht erreichbar sind. Dann vergeben wir diese Plätze kurz vor Kursbeginn an Interessenten auf der Warteliste, um eine volle Auslastung der verfügbaren Terminals zu gewährleisten.

Die Vorbereitungen für eine Sonderausgabe der MITTEILUNGEN DES URZ mit dem Titel *Kursübersicht 1992* sind fast abgeschlossen. Diese Kursübersicht informiert Sie über die Kursinhalte sowie weitere Termin- und Kursangebote und erscheint voraussichtlich im April.

Ursula Riedel

TERMINE TERMINE TERMINE TERMINE TERMINE

28. April 92 10.00 Uhr Raum 1/017

Vortrag von *Herrn Hartwig* von IBM Deutschland zum Thema:

Desktop Publishing

Am 31. 3. 92 und 28. 4. 92 17.30 Uhr findet jeweils wieder der

Unix-Stammtisch in Sachsen

in der Mensa, Str. der Nationen statt.
(Bitte Mitte März bzw. Mitte April Aushänge beachten.)

Meldungen für die erste Veranstaltung bitte an Rosita Pudlat, URZ, Tel. 668 656